# Internship Project: Network Sniffer

Submitted by: Bharti

Internship Code: Alpha

# Objective

Build a Python-based network sniffer to analyze real-time traffic.

Understand IP, TCP/UDP protocols and visualize packet flow.

## Tools & Libraries

- Python 3.x
- Scapy
- FPDF
- python-pptx
- PIL

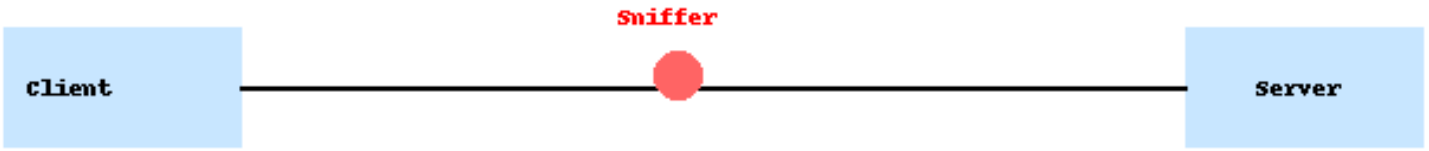
## Code Overview

- Define a packet processing function.
- Use `sniff()` to capture packets.
- Extract IP, TCP/UDP headers, decode payload.

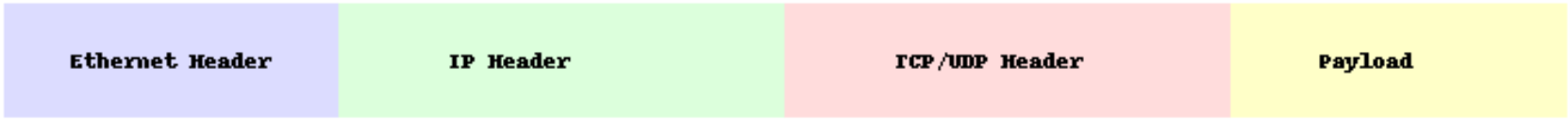
# Sample Code

```
from scapy.all import sniff, IP, TCP, UDP, Raw

def process_packet(packet):
    if IP in packet:
        print(f"{packet[IP].src} -> {packet[IP].dst} | Protocol: {packet[IP].proto}")
        if TCP in packet:
            print(f"TCP Port: {packet[TCP].sport} -> {packet[TCP].dport}")
        elif UDP in packet:
            print(f"UDP Port: {packet[UDP].sport} -> {packet[UDP].dport}")
        if Raw in packet:
            try:
                print(packet[Raw].load.decode(errors='ignore'))
            except:
                print('Raw payload could not be decoded')

sniff(filter="ip", prn=process_packet, store=0)
```

# Network Flow Diagram



# Packet Structure Diagram



## Use Cases

- Network troubleshooting
- Security monitoring
- Education
- Debugging protocols

## Challenges Faced

- Root permissions needed
- Packet volume handling
- Binary decoding
- Cross-platform support

# Learning Outcomes

- Gained experience with packet analysis
- Understood protocol headers
- Used Scapy effectively

# Acknowledgements

Grateful to Internship Code Alpha team and mentors for guidance and support.